REMARKS

In the Office Action, claims 1 - 20 were noted as pending in the application, and all claims were rejected. By this amendment, no claims have been amended, added, or canceled. Thus, claims 1 - 20 are pending in the application. The rejections of the Office Action are traversed below.

Rejection of Claims 1 - 6, 9, 10, 15, and 17 - 20 under 35 USC §103

In item 1, on pages 2 - 4 of the Office Action, claims 1 - 6, 9, 10, 15, and 17 - 20 were rejected under 35 USC § 103 as being unpatentable over published international patent application No. WO 99/01848 to Vatanen in view of published international patent application No. WO 97/50207 to Liljeqvist et al. This rejection is respectfully traversed.

As a threshold matter, Applicants note that in item 1, on page 2 of the Office Action, the above-referenced claims are allegedly rejected under both 35 USC §103(a) and 35 USC §102(b). However, because the Office Action expressly admits on page 2 that the Vatanen reference does not teach every feature recited at least in independent claim 1 and because a rejection under 35 USC §102 requires that a single reference teach all the features of a rejected claim, the Applicants presume the rejection beginning on page 2 was intended to be under 35 USC §103 alone.

The Claimed Invention

Exemplary embodiments of the Applicants' invention are directed to a system and method for executing secure data transfer between a communications device and an application server over a network. An agreement proposal for a secure transfer of data is sent from the server to a security adapter connected to the network, wherein the security adapter resides on the network distinctly from the server and the communications device. A message is created by and sent from the security adapter to the communication device to activate a signing application. The signing application signs the data, which is then sent from the communications device to the security adapter. The security adapter verifies the signature for the data and then sends the verified signed data to the server.

The Vatanen Reference

Vatanen discloses a procedure for the activation and/or closing of an application between a mobile station and an application control server, based on a key list maintained on the mobile station for determining whether the mobile station has a valid right of access to the application (Vatanen at abstract; page. 3, lines 14 - 25). Upon activation of an application stored in the mobile station's subscriber identity module (SIM), a message is sent from the application control server to the mobile station concerning the opening of the application, the message containing the application key to be used in the application (page, 4, lines 21 - 26; page 6, lines 21 - 26). When the user of the mobile stations accesses the application, the mobile station identifies itself to the application server by sending the keys needed to the application server to access the application (page 8, lines 10 - 17).

The Liljeqvist et al. Reference

Liljeqvist et al. discloses an Internet communication system including security means for ensuring that transactions between a World Wide Web server and an Internet client are secure (Liljeqvist et al. at abstract). A client-side security module (4) and a WWW-side security module (7) are utilized for encrypting and decrypting data transmitted between the WWW server and the Internet client (page 9, line 16 - page 10, line 8; Figs. 1 & 2). These two modules are also used to electronically sign the data to be transmitted and to verify the electronic signature of the received data (page 9, lines 19 - 21; page 10, lines 5 - 6).

The Claimed Invention is Patentably Distinguishable Over the Cited Documents

The Applicants' claimed invention is directed to a system and method for executing secure data transfer between a communications device and an application server over a network. In particular, and reciting independent claim 1, there is claimed a method for executing secure data transfer between a communication device and an application server, wherein data are transferred over a network between the application server and the communication device, including:

sending an agreement proposal for a secure transaction of data from the server to a security adapter connected to the network, said security adapter residing on the network distinctly from the server and the communication device,

3

creating and sending a message from the security adapter to the communication device in order to activate a signing application,

the signing application signing the data to be sent,

sending the signed data from the data from the communication device to the security adapter,

verifying the signature for the data, and

sending the verified signed data to the server for execution of the transaction.

The Office Action cites to the Vatanen reference for disclosing all the features recited in claim 1 except for the feature that the security adapter resides on the network distinctly from the server and the communication device. The Applicant respectfully asserts that the Office Action's reliance on Vatanen is misplaced. Vatanen merely discloses the activation process whereby a mobile station is authorized to access a remote application, such as communication with a bank process (Vatanen at abstract; page 3, lines 10 - 25). Contrary to the assertions of the Office Action, Vatanen fails to disclose the signing of any data whatsoever; nor does Vatanen disclose sending signed data or verifying the signature of transmitted data. Instead, Vatanen is limited verifying a user's right to remotely access an application (page 4, lines 14 - 17). Vatanen discloses sending a set of validation keys from an application control server to be stored on the SIM card of the mobile station (page 3, lines 10 - 14; page 6, lines 20 - 26). When the mobile station wants to access the secured application, the mobile station sends to the bank via the application control server the keys needed to use the application (page 8, lines 10 - 15). Upon verification that the keys are correct, the mobile station is granted access to the application (page 8, lines 16 - 17).

The Office Action admits that Vatanen fails to disclose that the security adapter of the present claimed application resides distinctly from the server and the communication device and cites to the Liljeqvist reference to allegedly disclose this feature. However, Liljeqvist et al. fails to remedy the deficiencies of the Vatanen because Liljeqvist et al. also fails to disclose the claimed features of the present security adapter. The security adapter recited in claim 1 has the features of:

receiving an agreement proposal for a secure transaction of data from a server, the security adapter residing on the network distinctly from the server and the communication device;

4

creating and sending a message to the communication device to activate a signing application;

receiving the signed data from the communication device;

verifying the signature for the data; and

sending the verified signed data to the server.

The Office Action is not clear regarding which element of Liljeqvist et al. allegedly corresponds to the present claimed security adapter, but the security module (7) of Fig. 2 appears to be the closest match to the present security adapter because the security module (7) is the only element of Liljeqvist et al. that has the ability to verify an electronic signature (Liljeqvist et al. at page 10, lines 3 - 6). However, beyond verifying an electronic signature of transmitted data, there is little similarity between the recited security adapter of claim 1 and the security module (7) of Liljeqvist et al. First, claim 1 recites that the security adapter receives an agreement proposal from the server, and that the security adapter creates and sends a message to the communication device in order to activate a signing application. Liljeqvist et al. fails to disclose any such features. Instead, the data being sent from the Internet client is automatically electronically signed for security purposes with no such messaging from the security module (7) (see Liljeqvist et al. at page 10, line 11 - page 11, line 10). Second, claim 1 expressly recites that the security adapter resides on the network distinctly from the server and the communication device (see, for example, Fig. 1). Liljeqvist et al., in contrast, discloses the security module (7) residing behind the WWW server, wherein all communications with the security module (7) must pass through the WWW application server, whether the communications are with the Internet client (1) or the application systems (10) (see Liljeqvist et al. at page 10, lines 2 - 5; Fig. 2).

Therefore, the Applicants respectfully submit that the Vatanen/Liljeqvist et al. combination fails to render obvious the features recited in independent claim 1.

While teachings of several documents may be combined to render a claimed invention obvious, there must be a motivation or suggestion in the documents relied upon to make the specific combination. The Office Action asserts on page 3 that it would have been obvious to modify Vatanen with the teachings of Liljeqvist et al. to provide more flexibility while meeting different levels of security. However, Vatanen is directed to a procedure for authenticating access to an application, based on a set of keys provided from an application

control server to a mobile station and is completely silent regarding multiple levels of security (Vatanen at abstract). The mobile station is either granted access to the application or it is refused access. Accordingly, the person of ordinary skill in the art and in possession of the teachings of Vatanen would not be motivated to provide for multiple levels of security and would not be motivated to modify Vatanen with the security module (7) features of Liljeqvist. At the very best, the Vatanen/Liljeqvist et al. combination would be the application access procedure of Vatanen with a remote, server-based security module (7) for verifying the proper keys for accessing the desired application. Even this combination, as discussed above, would fail to render obvious all of the features recited in independent claim 1 herein.

For the reasons discussed above, claim 1 is believed to be patentably distinguishable over Vatanen and Liljeqvist et al., whether taken alone or in combination. Accordingly, it is respectfully requested that the rejection of claim 1 be withdrawn.

Independent claims 9, 17, 18, and 19 recite subject matter similar to the features recited in claim 1 and are patentably distinct over Vatanen and Liljeqvist et al. for the same reasons as presented above regarding claim 1.

Claims 2 - 6 depend from claim 1 and include all the features of claim 1 plus additional features which are not taught or suggested by the Vatanen and Liljeqvist et al. documents. For example, claim 6 specifies sending the agreement proposal for the secure transaction from the server to the communication device for acceptance before the agreement proposal is sent to the security adapter, which is neither taught nor suggested by Vatanen or Liljeqvist et al. The Office Action cites to Vatanen at page 6, lines 11 - 20 as allegedly disclosing this feature. However, the cited portion of Vatanen discloses a step of the mobile station setup procedure whereby the background bank system sends an identifier corresponding to the mobile station's SIM card to an application-specific card control system. The card control system sends an opening message to the SIM card corresponding to the identifier, the opening message containing the customer's user key for ultimately accessing the bank services when the customer so desires (Vatanen at page 6, lines 20 - 29). Therefore, for at least this reason and the reasons set forth above with respect to claim 1, it is submitted that claims 2 - 6 patentably distinguish over the Vatanen and Liljeqvist et al. documents.

Claims 10 and 15 depend from claim 9 and include all the features of that claim plus additional features. Therefore, for at least the reasons set forth above with respect to claim 9,

6

it is submitted that claims 10 and 15 patentably distinguish over the Vatanen and Liljeqvist et al. documents.

Claim 20 depends from claim 19 and includes all the features of that claim plus additional features. Therefore, for at least the reasons set forth above with respect to claim 19, it is submitted that claim 20 patentably distinguishes over the Vatanen and Liljeqvist et al. documents.

Rejection of Claims 7, 8, and 11 - 14 under 35 USC §103

In item 1, on pages 4 - 6 of the Office Action, claims 7, 8, and 11 - 14 were rejected under 35 USC § 103 as being unpatentable over Vatanen and Liljeqvist in view of U.S. Patent No. 6,463,534 to Geiger et al. and further in view of international published application No. WO 98/57511 to Sandgren et al. This rejection is respectfully traversed.

The Geiger et al. Patent

Geiger et al. discloses a system and method for conducting transactions in a wireless commerce system, wherein an attribute certificate is delivered across a wireless network from an attribute authority to a wireless device (Geiger et al. at abstract; Col. 1, lines 33 - 42). The attribute authority is verified on the wireless device using the delivered attribute certificate and a root public key certificate pre-loaded in the wireless device (abstract; Col. 1, lines 42 - 45). An attribute is delivered to the wireless device over the wireless network, and the attribute is enabled at the wireless device (abstract; Col. 1, lines 45 - 49). The wireless device can then authorize a payment transaction for the attribute from the attribute authority (Col. 1, lines 50 - 54).

The Sandgren Reference

Sandgren discloses a system and method for activating and deactivating a locking function in a mobile terminal, wherein the locking function is activated and deactivated based on operator-executed commands transferred to the mobile terminal (Sandren at abstract; page 1, line 36 - page 2, line 7). The locking function can be unlocked by means of SIM toolkit functions and a carrier service, such as SMS or USSD (abstract; page 2, lines 9 - 12; page 3, lines 22 - 23). The unlocking can be controlled by different criteria, such as when the customer has transmitted a signed agreement to the network operator (abstract; page 3, lines

23 - 26).

The Claimed Invention is Patentably Distinguishable Over the Cited Documents

The Applicants' claimed invention is directed to a system and method for executing secure data transfer between a communications device and an application server over a network. Claims 7 and 8 depend from claim 1 and include all the features of claim 1 plus additional features which are not taught or suggested by the Vatanen, Liljeqvist et al., Geiger et al., or Sandgren documents. Claims 11 - 14 depend from claim 9 and include all the features of claim 9 plus additional features which are not taught or suggested by the Vatanen, Liljeqvist et al., Geiger et al., or Sandgren documents. Therefore, for at least the reasons set forth above with respect to claims 1 and 9, it is submitted that claims 7, 8, and 11 - 14 patentably distinguish over the Vatanen, Liljeqvist et al., Geiger et al., or Sandgren documents.

Rejection of Claim 16 under 35 USC §103

In item 2, on page 6 of the Office Action, claim 16 was rejected under 35 USC § 103 as being unpatentable over Vatanen and Liljeqvist in view of U.S. Patent No. 5,425,077 to Tsoi. This rejection is respectfully traversed.

The Tsoi Patent

Tsoi discloses a method for displaying and entering selected alphabetic labeled designations in the primary visual display of a mobile telephone (Tsoi at abstract). Upon entering a particular transaction with the mobile telephone, such as dialing a telephone number, a context-sensitive list of function labels are displayed on the mobile telephone (Col. 6, lines 10 - 15; Col. 6, line 66 - Col. 7, line 5; Figs. 5 & 7). Adjacent to each displayed function label is a corresponding soft-label key (Col. 6, lines 26 - 29; Fig. 5). Depressing a soft-label key will initiate the corresponding displayed function (Col. 7, lines 6 - 14; Figs. 5, 7, & 8).

The Claimed Invention is Patentably Distinguishable Over the Cited Documents

The Applicants' claimed invention is directed to a system and method for executing secure data transfer between a communications device and an application server over a

network. Claim 16 depends from claim 9 and includes all the features of claim 9 plus additional features which are not taught or suggested by the Vatanen, Liljeqvist et al., or Tsoi documents. For example, claim 16 recites that the mobile phone comprises means for displaying a particular icon, wherein the user can be assured that he is really communicating directly with the security application. The Office Action cites to Tsoi at Col. 6, lines 1 - 17 as allegedly disclosing this feature. However, the cited portion of Tsoi is merely a description of Fig. 5 of the Tsoi patent, where a mobile telephone is shown, with the context sensitive function labels of LAST, MEMORY, and MENU are displayed adjacent to their respective soft-label keys 82, 84, and 86. Tsoi is completely silent regarding communicating with any security application whatsoever. Instead, Tsoi is directed to providing labeled function keys to simplify the process of using a mobile phone (Tsoi at Col. 2, lines 41 - 46). Therefore, for at least this reason and the reasons set forth above with respect to claim 9, it is submitted that claim 16 patentably distinguishes over the Vatanen, Liljeqvist et al., and Tsoi documents.

Summary

It is submitted that none of the documents, either taken alone or in combination, teach the claimed invention. Thus, claims 1 - 20 are deemed to be in a condition suitable for allowance. Reconsideration of the claims and an early Notice of Allowance are earnestly solicited. If any fees are required in connection with this Amendment, please charge the same to our Deposit Account No. 02-4800.

Respectfully submitted,

Burns, Doane, Swecker & Mathis, L.L.P.

By:_____
William N. Hughet
Reg. No. 44,481

P.O. Box 1404
Alexandria, Virginia 22314-0404
Telephone: (703) 836-6620
Facsimile: (703) 836-2021

Date: September 21, 2004   .

VA 378768.1

9